siam news

SIAM News Blog **RESEARCH**

Mathematical Structures within Blockchain and Decentralized Finance

December 09, 2022 By Zachary Feinstein

Humans interact with decentralized products every day, whether we realize it or not. Decentralized encyclopedias (like Wikipedia) regularly supply us with information, and social media serves as a decentralized news aggregator. Decentralization has also reached the realm of finance under the veil of *blockchain*. Yet while an incorrect factoid in an encyclopedia may be frustrating but can be corrected, the verification of financial transactions in a crowd is a massive undertaking in which errors cost real money.

Satoshi Nakamoto (a presumed pseudonym) proposed blockchain as a distributed ledger and consensus mechanism to handle the verification process for financial transactions [5]. In the years since Bitcoin's introduction, individuals have made and lost massive amounts of wealth in the cryptocurrency and broader decentralized finance (DeFi) space.

A financial asset is broadly defined as any object with a value that one can trade or use as an investment, such as stocks, bonds, or commodities (e.g., oil and gold). Digital assets are similar but exist solely as computer data — unlike physical assets, such data is easy to copy. Maintaining a single ledger (i.e., database) of ownership at a trusted bank, exchange, and so forth can overcome this issue, so long as one trusts that the institution will not suffer a catastrophic failure through hacking, financial collapse, or other means.

As a distributed ledger, blockchain is a trustless database. It moves assets onto a *public* digital ledger (i.e., tokenizing assets) and thus makes an entire ecosystem of new investments—including market making and insurance underwriting—available to investors. Users can easily manipulate digital assets with computer code, allowing so-called *smart contracts* to automate complex transactions and providing the foundation of DeFi.

Distributed Ledger Technology and Consensus Mechanisms

As its name indicates, blockchain is quite literally a chain of data blocks that are added sequentially over time. For financial data, these blocks represent financial transactions (e.g., I send $10 to you). One can therefore verify any new transaction by examining the prior state of the entire world (do I have $10 to send to you?). Since anyone may read the entire blockchain, the whole system can verify the new data and reject any fraudulent data.

Cryptography (the "crypto" of cryptocurrency) secures the sequence of transactions, and each block holds a hash code of the prior block in the system (see Figure 1). If earlier data were modified, this hash would become inaccurate and the attack on the data would be detectable. As such, blockchain data is often referred to as immutable.

Satoshi Nakamoto's original proposal for Bitcoin presented blockchain in a proof of work system [5]. At its most basic level, proof of work constructs the blockchain through the competition of miners who attempt to solve a cryptographic problem as quickly as possible. The miners seek a hash code for the new block that begins with a specific number of zeros; a higher number of zeros makes the hashing problem increasingly more difficult and necessitates progressively more computational resources. The solution of proof of work requires significant (and redundant) computational resources because all miners compete to find a solution. Any mathematical insights that help efficiently solve these hashing problems can yield significant profits.

Other consensus mechanisms reduce the environmental impacts of proof of work. The most common alternative mechanism is proof of stake, which is utilized by the Ethereum blockchain. In contrast to the competition in proof of work, proof of stake obliges miners to provide collateral that can be taken away if they act in bad faith; in exchange, a miner is randomly chosen (based on the quantity of collateral) to receive the rewards from minting the next block.

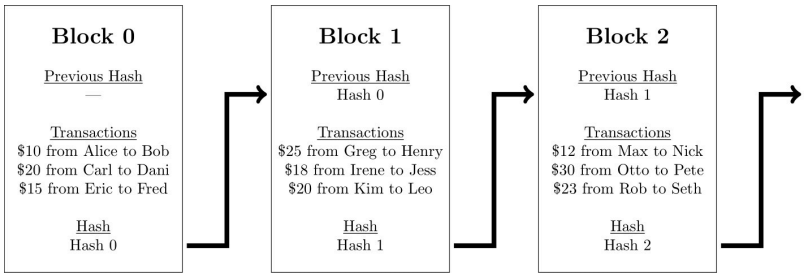

Figure 1. Stylized visualization of a blockchain. Figure courtesy of Zachary Feinstein.

Stablecoins and Central Bank Digital Currencies

The recent "crypto winter" began with the crash of UST, a stablecoin that lost its peg to the U.S. dollar. Unlike this scenario, stablecoins are meant to serve as a digital asset that lacks the kind of volatility that hinders the broad adoption of cryptocurrency for common transactions.

There are two fundamental types of stablecoin: custodial and algorithmic [4]. Algorithmic stablecoins are especially prone to losing their peg, as evidenced by the collapse of Terra Luna/UST in May 2022.

As a potential alternative to stablecoin, central banks around the world are presently exploring the possible production of their own digital assets. These central bank digital currencies (CBDCs), which are backed by the faith and credit of the nation, provide the same level of security as fiat currencies.

One can construct CBDCs as either a central bank account token or digital cash [6]. Central banks currently allow certain privileged institutions to hold accounts in all major economies. When opened to individuals, such a structure would represent a new safe and interest-bearing asset. However, this construction could cause financial instability as depositors reduce their investments at private banks [3]. CBDCs also generate privacy concerns because the central bank would be privy to a ledger of all digital transactions.

In contrast, the digital cash structure for CBDCs provides individuals with more privacy. Bank accounts would hence be augmented to hold both physical cash and an electronic wallet for CBDC. Depositors could then freely convert these forms of cash via commercial banks. Though it would function much like a debit card, this system—with the proper cryptographic structures—would allow one to spend digital cash without revealing the counterparties, which is an important characteristic of cash.

Decentralized Exchanges and Automated Market Makers

The earliest and most traditional way for an individual to invest in digital assets was through centralized exchanges. Investors would specify desired transactions (e.g., buying if the price drops or selling if the price rises) in a centralized order book, and market orders would subsequently be implemented based on this book. But centralized exchanges are vulnerable to hackers and/or catastrophic failures, both of which could cause individuals to lose their entire investments; the 2014 collapse of the Bitcoin exchange Mt. Gox, the sudden implosion of FTX in 2022, and the hacks of Coincheck and KuCoin are pertinent examples.

Automated market makers (AMMs) are a specific class of decentralized market makers that act as a source of liquidity against which anyone can trade. Solving simple mathematical equations sets the price and maintains AMM reserves at an equilibrium [1]. If u is a utility function for an AMM, investors can then trade along this indifference curve. In short, provided that two assets exist for which the AMM respectively holds $a, b > 0$ of the assets, one can exchange $x > 0$ units of the first asset for y units of the second, where

$$u(a + x, b - y) = u(a, b).$$

The prototypical AMM is Uniswap V2, which corresponds to a logarithmic utility function $u(a, b) = \log(a) + \log(b)$ (this equation is more commonly written such that the utility is the product of asset reserves; these formulations have equivalent indifference curves). This logarithmic utility is also used by SushiSwap, DeFi Swap, QuickSwap, and other decentralized exchanges.

People use many other formulas beyond Uniswap V2 in practice. For instance, mStable utilizes a linear utility function $u(a, b) = a + b$ to provide a stable price point. This construction only offers limited liquidity, as the AMM can run out of assets when the market price point differs from the AMM's offered price. However, alternative current AMMs—such as StableSwap and Curve—are a combination of Uniswap V2 and mStable. In this way, they provide more liquidity to the market than mStable but concentrate that liquidity around a smaller range of prices than Uniswap V2. Uniswap V3—an update to Uniswap V2—notably allows for concentrated liquidity while maintaining a similar utility function.

Like with traditional market makers, AMMs earn fees on each trade as compensation for providing liquidity against which investors can trade. And as with other areas of DeFi, investors can post their own assets to AMMs to earn a fraction of the fees that are captured by this trading activity. In practice, these fees are applied as a fixed fraction of the assets that are bought or sold. But poorly designed fee structures implicitly subsidize large (bulk) transactions, while others prefer a sequence of small trades. For instance, one study reported that the appropriate fee structure should be defined as a differential equation with respect to the prevailing market price [2]. That is, for each marginal asset that is bought or sold, a fraction of the marginal price is taken as a fee.

In addition to earning fees, posting liquidity to an AMM increases the size of available assets and decreases the price impacts from trading; i.e., progressively larger amounts of available liquidity yield increasingly smaller impacts from any individual trade. AMMs can thus create large, *decentralized* liquidity pools that serve as functional markets for digital assets.

The Future of Decentralized Finance

Blockchain has the potential to democratize finance by replacing traditional (centralized) intermediaries with a distributed ledger. This novel technology introduces the possibility of radically new financial constructions that can lower the barrier of entry for innovative products. However, improper understanding of the underlying models and risks that are inherent in these ventures can kill DeFi in its cradle. After all, irrational exuberance gave way to the ongoing crypto winter. The future of DeFi requires that we study what has come before as well as what has yet to transpire.

References

[1] Angeris, G., & Chitra, T. (2020). Improved price oracles: Constant function market makers. In *Advances in financial technologies 2020 (AFT '20): Proceedings of the 2nd ACM conference on advances in financial technologies* (pp. 80-91). New York, NY: Association for Computing Machinery.
[2] Bichuch, M., & Feinstein, Z. (2022). Axioms for automated market makers: A mathematical framework in fintech and decentralized finance. Preprint, *arXiv:2210.01227*.
[3] Bindseil, U., Panetta, F., & Terol, I. (2021). *Central bank digital currency: Functional scope, pricing and controls.* (European Central Bank Occasional Papers Series, No. 286). Retrieved from https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op286~9d472374ea.en.pdf?2dfe373fb889c60a88fa65393caa5255.
[4] Grasselli, M.R., & Lipton, A. (2021). Cryptocurrencies and the future of money. Preprint, *arXiv:2109.10177*.
[5] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf.
[6] Summer, M., & Hermanky, H. (2022). A digital euro and the future of cash. *Oesterreichische National Bank*. Retrieved from https://taler.net/papers/digital-euro-and-the-future-of-cash.pdf.

About the Author

Zachary Feinstein

Assistant Professor, Stevens Institute of Technology

Zachary Feinstein is an assistant professor in the School of Business at Stevens Institute of Technology. His research lies at the intersection of financial mathematics and financial technology.